SECTION II: REMARKS

A. Summary of Amendments to the Claims

By the present amendment, independent claims 1, 18, and 20 have each been amended to recite (*inter alia*) "wherein the control commands are separately transmitted each time the electronic application renders the electronic content accessible to the user, the method comprising maintaining a count of a number of times that the control commands for rendering the electronic content accessible to the user are transmitted." Such language clarifies that the count relating to transmission of control commands specifically embodies the number of times that such commands are transmitted to benefit the specific user (i.e., by rendering electronic content accessible to that user). Such amendments are supported by the originally-filed disclosure, for example, at original claim 3 (referring to count of number of times that control commands are transmitted to a specific portable wireless device). No new matter within the meaning of 35 U.S.C. 132(a) has been introduced by the foregoing amendments.

B. The Claim Rejections Under 35 U.S.C. 103(a) Should Be Withdrawn

The February 26, 2010 Office Action contained numerous rejections under 35 U.S.C. 103(a), namely:

- a rejection of claims 1, 11, 14, 18, 20-28, and 32 as allegedly being unpatentable for obviousness over U.S. Patent Application Publication No. 2001/0016834 to Yamanaka et al. ("Yamanaka") in view of U.S. Patent Application Publication No. 2003/0046548 to Brown et al. ("Brown"), further in view of U.S. Patent Application Publication No. 2007/0101139 to Bayer ("Bayer");
- a rejection of claims 2 and 15-17 as allegedly being unpatentable for obviousness over Yamanaka, Brown, and Bayer, and further in view of U.S. Patent No. 6,874,018 to Wu ("Wu");

- a rejection of claims 4 and 29-31 as allegedly being unpatentable for obviousness over Yamanaka, Brown, Bayer, and Wu, and further in view of U.S. Patent Application Publication No. 2004/0220926 to Lamkin et al. ("Lamkin");
- a rejection of claims 10 and 34 as allegedly being unpatentable for obviousness over Yamanaka, Brown, and Bayer, and further in view of Lamkin;
- a rejection of claims 6-8 as allegedly being unpatentable for obviousness over Yamanaka, Brown, Bayer, and Wu, and further in view of Lamkin;
- a rejection of claims 12-13 and 19 as allegedly being unpatentable for obviousness over Yamanaka, Brown, and Bayer, and further in view of U.S. Patent Application Publication No. 2004/0003398 to Donian et al. ("Donian");
- a rejection of claim 9 as allegedly being unpatentable for obviousness over Yamanaka, Brown, Bayer, and Lamkin, and further in view of Donian; and
- a rejection of claims 5 and 33 as allegedly being unpatentable for obviousness over Yamanaka, Brown, Bayer, and Wu, and further in view of U.S. Patent Application Publication No. 2004/0031377 to Ochiyama et al. ("Ochiyama")

Such rejections are traversed.

Claims 1, 2, and 4-34 are pending in the above-identified application, with claims 1, 18, and 20 being independent claims, and the balance of claims depending (whether directly or indirectly) on one of claims 1, 18, or 20.

Amended independent claims 1, 18, and 20 each require (*inter alia*) separate transmission of control commands each time the electronic application renders the electronic content accessible to the user, and maintaining a count of a number of times that the control commands for rendering the electronic content accessible to the user are transmitted.

Yamanaka discloses a network-based digital content billing system that enables use of digital content by a user if the user selects and views advertisements. An administrator contracts with an advertiser and a holder holding rights to let a third person use digital content. A holder of rights for use of digital content sets the digital content to become usable by using an execution key, downloads the execution key to an administrator through a network, and downloads the digital content not made usable to a

distributor through the network. The distributor downloads the digital content to a user through the network. When the user sends an execution declaration of the digital content to the administrator, the administrator downloads the execution key and an advertising information piece received from the advertiser to the user through the network. The user can therefore use the digital content made usable by the execution key while seeing the advertising information piece. The administrator collects an advertising rate corresponding to the number of execution times of the digital content from the advertiser and pays to the holder an execution fee corresponding to the number of times of execution of the digital content.

Yamanaka discloses that digital content is converted into encrypted form ("digital information ciphering type") via a distribution server prior to transmission to the user. See, e.g., Yamanaka, ¶ [0113][1]. Yamanaka disclosed that the ciphered digital content is then deciphered in the user's terminal using a decryption key. (Id.) Since Yamanaka's digital content is ciphered prior to transmission to the user, there is no need (and indeed no purpose) for Yamanaka to provide a user with an electronic application that restricts user access to storable user content. Yamanaka therefore fails to disclose or suggest the feature of "providing an electronic application to the user that restricts user access to the storable electronic content" as recited in Applicant's independent claims 1 and 18. Yamanaka similarly fails to disclose or suggest "a service[,] that is separate from the device that provides control commands to the application[,] for controlling access to content from the medium when inserted in the media drive" as recited in Applicant's independent claim 20.

Since Yamanaka fails to disclose an electronic application provided to the user that restricts user access to storable electronic content, Yamanaka also fails to disclose control commands enabling such an electronic application to render the electronic content accessible to the user, as recited in Applicant's independent claims 1 and 18.

[1] "[0113] FIG. 3(a) is a diagram showing a preventing method of digital content unrighteous execution in which digital content converted into a digital information ciphering type is distributed. In FIG. 3(a), **digital content is ciphered in the server 41a of the distributor 4a by using the encryption key and is downloaded to the terminal 11a of the user 1a**. Thereafter, the ciphered digital content is deciphered in the terminal 11a of the user 1a by using a decryption key, and the deciphered digital content is used by the user 1a.

Further with respect to claim 20, since Yamanaka discloses access to content only via download to a user (rather than control of access to content inserted into a media drive of a device), and Yamanaka fails to disclose an application that accesses content from a medium inserted in the media drive, Yamanaka fails to disclose utilization of "an application that accesses content from a medium inserted in the media drive" and "a service separate from the device that provides control commands to the application for controlling access to content from the medium when inserted in the media drive" as required by claim 20.

In the February 26, 2010 Office Action at page 4, the examiner conceded that Yamanaka does not teach the user playing electronic advertising content, and further conceded that Yamanaka fails to teach maintaining a count of a number of times that control commands are transmitted.

Brown discloses an apparatus and method in which access rights information (e.g., access rights tags or metadata) is provided in association with information and content such that use of the information and content is controlled based on the access rights information. Such "access rights information may be used to control access to content, identify how access to content may be obtained, monitor or keep a record of access to the content[2]." An avowed purposes of Brown is to provide protections against unauthorized use of information and content (e.g., copyrighted material available via a web site) in a distributed computing environment[3].

At paragraph [0034] thereof, Brown states:

> "Each of the client devices 108-112 are preferably equipped with browser applications that either include in the code of the browser application, or in plugin applications to the browser application, software code for making use of access rights information (ARI) in accordance with the present invention. The ARI provides information to the browser application or plugin application regarding the various functions that may be performed on the content associated with the ARI. In other words, the ARI controls the way in which the content may be used by users of client devices to which the content is provided."

[2] Brown, ¶ [0010].
[3] Brown, ¶¶ [0006]-[0007].

Brown discloses that a server receives a request for content from a client device and provides the requested content, if possible, along with the associated ARI to the client device[4]. Based on the processing of the ARI, various functions may be enabled and/or disabled in the web browser application[5]. The ARI may therefore be used by providers of content to control the way in which the content may be used by receivers of the content[6]. The invention according to Brown provides a mechanism by which access rights may be assigned to information and content in a manner that allows browsers to limit use of the information and content based on the assigned access rights[7]. Various levels of access rights may be granted to different users[8]. User access level information may be stored in a data structure associated with a server in which a web page resides, stored on a client device, or distributed across multiple servers and/or client devices[9].

Brown discloses that an "ARI tag may be used as a mechanism for gate keeping access to associated content by requiring the user to 'pay' for access by viewing or interacting with an advertisement or the like. … If the user clicks on the advertisement, the user is presented with the advertisement, redirected to an associated web site, or the like. Once the required viewing or interaction with the advertisement is complete, the user's access level may be temporarily increased, via the access levels defined in the ARI tag associated with the image, so that the user may view the image. In this way, the ARI tag defines the manner by which a user may earn access to associated content[10]." Brown similarly discloses in one example that "the ARI tag may indicate that the user must click on and view an advertisement before access is provided to the electronic mail message. The level of the user's interaction with the advertisement or an associated advertiser's web page may be configurable using the access levels defined in the ARI tag[11]."

Nothing in Brown discloses that "control commands are separately transmitted each time the electronic application renders the electronic content accessible to the user" as required by Applicant's independent claims 1, 18, and 20. Instead, Brown discloses

---

[4] Brown, ¶ [0036].
[5] Brown, ¶ [0037].
[6] Id.
[7] Brown, ¶ [0048].
[8] Brown, ¶¶ [0062]-[0064].
[9] Brown, ¶ [0066].
[10] Brown, ¶¶ [0104]-[0105].
[11] Brown, ¶ [0107].

that a user's access level may be temporarily increased for some indeterminate time[12], or that a user may accrue points to change access level[13]. Neither of these procedures compel separate transmission of control commands each time the electronic application renders the electronic content accessible to the user.

With respect to Applicant's claim 20, since Brown discloses access to content only via download to a user (rather than control of access to content inserted into a media drive of a device), and Brown fails to disclose an application that accesses content from a medium inserted in the media drive, Brown fails to disclose utilization of "an application that accesses content from a medium inserted in the media drive" and "a service separate from the device that provides control commands to the application for controlling access to content from the medium when inserted in the media drive" as required by claim 20.

In the February 26, 2010 Office Action at page 4, the examiner conceded that Brown (as well as Yamanaka) fails to teach maintaining a count of a number of times that control commands are transmitted.

In seeking to remedy the failure of both Yamanaka and Brown to teach maintaining a count of a number of times that control commands are transmitted, the examiner alleged that Bayer teaches that "control commands are separately transmitted each time the electronic application renders the electronic content accessible to the user" and "maintaining a count of a number of times that the control commands are transmitted[14]."

Bayer discloses a system for distributing electronic surveys and similar information, including a web site addressable by one or more client computer systems for connecting to the content protection system over the Internet or other public network. Viewer software is installed at the client computer and generates unique viewer identification information that is used for registering the viewer with a respondent. Based on a survey invitation, a client computer may be used to participate in a survey transmitted by a server. The client computer system enables the content viewer to connect to the web site of the content protection system and download a file with

[12] Brown, ¶ [0105].
[13] See, e.g., Brown, ¶ [0103].
[14] February 26, 2010 Office Action, page 4.

encrypted content information for that survey. The viewer software sends a request to the content protection system for a key to decrypt the downloaded content information. Based on various criteria, including whether the survey has yet been taken by a user at the client computer, a decryption key is sent to the client computer system and the viewer uses the key to decrypt the encrypted content information file for viewing thereof. During viewing, the viewer ignores interrupts from the keyboard and mouse which typically allow the user to access information and thereby enable copying, such as a print screen key, right mouse button, or screen scraper. If the user selects another window other than the window of the viewer, the viewer stops showing the decrypted content and displays a protection image in its place. Thus, the content information is protected from authorized viewing by encryption and protected from unauthorized copying by limiting the ability of the user access to only viewing. (Bayer, ¶¶ [0010]-[0011].) A primary purpose of Bayer is to enable conduction of surveys over the Internet in which content information of the survey is protected from unauthorized viewing or copying. (Bayer, ¶¶ [0003]-[0006].)

In support of the examiner's allegation that Bayer discloses "control commands are separately transmitted each time the electronic application renders the electronic content accessible to the user" and "maintaining a count of a number of times that the control commands are transmitted," the examiner pointed to paragraph [0037] of Bayer, which states:

> "After sending the key, if a record exists in the View Content table 26 for the ContentID, SurveyID, and RespondentID of the request, the Key server increments the count value by one, otherwise the Key server adds a record in the View Content table for the ContentID, SurveyID, and RespondentID and the count value is set to one."

Discussion of the definitions of terms in the preceding excerpt is warranted, with reference to Bayer Figure 3 (reproduced below).

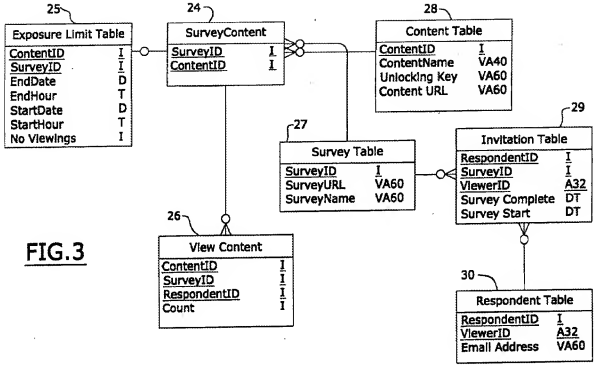

FIG.3

Bayer paragraph [0023], which refers to FIG. 3, states:

> [0023] Records of multiple tables are stored in database 20 shown in FIG. 3. The records of the Exposure Limit 25 and **ContentView 26 tables store exposure limit information.** The records of the Respondent table 30 store registration information. The records of the Survey 27 and Invitation 29 tables store survey and invitation information. The records of the SurveyContent 24 and Content 28 tables store the information regarding the content files. Each table is related to each other by one or more identifiers defined as follows: **ContentID is an identifier to an encrypted content file**; **SurveyID is the identifier of a particular survey**; **RespondentID is an identifier for an invitation** to take a survey or view secure content; **ViewerID is an identifier which uniquely identifies a client computer system** for an instance of the viewer software downloaded to a client computer system. The **RespondentID need not be unique, but when combined with the ViewerID may be considered unique in representing a survey participant**.

The foregoing passage in combination with Figure 3 provides context to Bayer paragraphs [0035] and [0037] as cited by the examiner relating to the "Count." Excerpts

of paragraphs [0035] and [0037] of Bayer are reproduced below along with comments relating to same.

Excerpt from Bayer	Comment
[0037] … After sending the key, if a record exists in the View Content table 26 for the ContentID, SurveyID, and RespondentID of the request, the Key server increments the count value by one, otherwise the Key server adds a record in the View Content table for the ContentID, SurveyID, and RespondentID and the count value is set to one. Thus, condition 1 confirms matching of ID's to that of the request to identify preselected invited survey participants, while conditions 2-4 represent examples of business rules to authorize sending of the key.	*ContentID* refers to an encrypted content file[15]. *SurveyID* refers to a particular survey[16]. *RespondentID* refers to an invitation to take a survey or view secure content[17]. **None of the foregoing three concepts refers to any specific survey participant (or user).** Instead, Bayer states that only *the combination of RespondentID and ViewerID* may be considered unique in representing a specific survey participant[18].
[0024] The Exposure Limit Table 25 has records with the following data fields: ContentID; SurveyID; EndDate …; EndHour …; StartDate …; StartHour …; and **No Viewing**, a number indicating the number of times the encrypted file associated with the ContentID can be viewed by a client computer system. .	The "NoViewing" data field reflects a maximum aggregate number of times that encrypted content (namely, a survey) can be viewed across an entire client computer system - without regard to any specific user (e.g., as could be identified by ViewerID). .
[0035] [*Condition 3*] if a record is present in the View Content table 26 having the ContentID, SurveyID, and RespondentID of the request, that the **Count field of the record is less than the No Viewing field** of the record in the Exposure Limit table 25 for the ContentID and SurveyID of the request	The passage bolded at left clarifies that the function of the Count field is to track the number of authorized survey participants, as compared to the NoViewing data field (i.e., aggregate total number of times that encrypted content (namely, a survey)can be viewed across an entire client computer system).

[15] Bayer, ¶[0023].
[16] Id.
[17] Id.; see also Bayer paragraph [0025], which states: "For a survey, multiple records are provided in the Invitation table 29 for the survey's SurveyID, where each record has a ViewerID associated with a particular client computer system and a RespondentID associated with the ViewerID for that survey. In this manner, the participants are selected for a survey. This selection may be made randomly from the pool of records of the Respondent table 30 by server 14, or the administrative computer may select each of the participants from the records of the Respondent table." The foregoing excerpt clarifies that **an invitation alone is not sufficient to identify a specific participant, since a single invitation may be propagated to multiple ViewerIDs associated with the client computer system**.
[18] Bayer, ¶[0023].

The excerpts from Bayer and comments embodied in the foregoing table demonstrate that **Bayer's "Count" is not specific to any participant or user**; instead, Bayer's "Count" is based upon satisfaction of the criteria of *ContentID* (identifying encrypted content), *SurveyID* (identifying a particular survey), and *RespondentID* (referring to an invitation to take a survey) – of which none refer to a specific participant or user (i.e., as would require ViewerID, according to Bayer ¶[0023]).

As indicated previously, each of Applicant's independent claims 1, 18, and 20 have been amended to recite (*inter alia*) "maintaining a count of a number of times that the control commands for rendering the electronic content accessible to **the user** are transmitted." **No such step is disclosed or suggested by Bayer.** Bayer's "Count" is not specific to any specific user, but rather tracks a number of authorized participants associated with a client computer system (e.g., for comparison to the "NoViewing" data field reflecting a maximum aggregate number of times that encrypted content can be viewed across an entire client computer system) – without regard to any specific user.

For at least the reason that the examiner has conceded that neither Yamanaka nor Brown disclose maintaining any count relating to transmission of control commands, and it has been demonstrated herein that Bayer fails to disclose "maintaining a count of a number of times that the control commands for rendering the electronic content accessible to the user are transmitted" as required by each of Applicant's amended independent claims 1, 18, and 20, the rejections of such claims under 35 U.S.C. 103 premised on Yamanaka, Brown, and Bayer should be withdrawn.

Moreover, a primary aspect of Bayer's invention is to cause electronic content to be inaccessible to the user whenever the user selects another window other than the window of the viewer[19]. Yet Bayer discloses that playing of restricted content may be resumed by the user when the "user click[s], via the mouse, on the viewer window[20]", without requiring re-transmission of control commands. Such disclosure by Bayer does

[19] See, e.g., Bayer, ¶[0011]: " During viewing, the viewer ignores interrupts from the keyboard and mouse which typically allow the user to access information and thereby enable copying, such as a print screen key, right mouse button, or screen scraper. **If the user selects another window other than the window of the viewer, the viewer stops showing the decrypted content and displays a protection image in its place.** Thus, the content information is protected from authorized viewing by encryption and protected from unauthorized copying by limiting the ability of the user access to only viewing."
[20] Bayer, ¶[0039].

not embody "separate transmission of control commands each time the electronic application renders the electronic content accessible to the user" as required by Applicants' claims 1, 18, and 20. That is, clicking of a mouse to render content accessible does not embody "separate transmission of control commands" that are "receivable from a party other than the user and that are generated upon the user selecting and playing the electronic advertising content" within the meaning of Applicant's independent claims 1, 18, and 20. This provides another reason why Bayer is inapposite to the subject matter of Applicant's claims.

It is therefore clear that Bayer does not disclose either (a) maintaining a count of a number of times that the control commands for rendering the electronic content accessible to the user are transmitted, or (b) separate transmission of control commands each time the electronic application renders the electronic content accessible to the user. The examiner conceded that Yamanaka and Brown fail to disclose the foregoing features in combination. None of the other references cited in the February 26, 2010 Office Action remedy the foregoing deficiencies of Yamanaka, Brown, and Bayer in disclosing the combination of (a) maintaining a count of a number of times that the control commands for rendering the electronic content accessible to the user are transmitted, and (b) separate transmission of control commands each time the electronic application renders the electronic content accessible to the user, as required by Applicants' independent claims 1, 18, and 20. Indeed, no reference other than Bayer was alleged by the examiner to embody separate transmission of control commands each time the electronic application renders the electronic content accessible to the user, and maintaining a count of a number of times that the control commands are transmitted.

Because the cited art fails to embody all the features recited in Applicants' independent claims 1, 18, and 20, withdrawal of the rejections of such claims under 35 U.S.C. 103 is warranted, and is respectfully requested.

Additionally, because dependent claims inherently include all of the features of the claims on which they depend[21], dependent claims 2, 4-17, 19, and 21-34 are patentably distinguished over the cited art for at least the same reasons as presented

[21] 35 U.S.C. 112, fourth paragraph.

hereinabove with respect to independent claims 1, 18, and 20. Accordingly, withdrawal of the rejections of dependent claims 2, 4-17, 19, and 21-34 is warranted, and is respectfully requested.

CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now-pending claims are in condition for allowance. Favorable examination of all pending claims and issuance of a notice of allowance are earnestly solicited. Should any issues remain that may be amenable to telephonic resolution, the examiner is invited to telephone the correspondent attorney listed below to resolve such issues as expeditiously as possible.

In the event there are any errors with respect to the fees for this response or any other papers related to this response, the Director is hereby given permission to charge any shortages and credit any overcharges of any fees required for this submission to Deposit Account No. 14-1270.

Respectfully submitted,

By: /vincent k. gustafson/
Vincent K. Gustafson
Registration No.: 46,182

INTELLECTUAL PROPERTY/
TECHNOLOGY LAW
P.O. Box 14329
Research Triangle Park, NC 27709

Dated: April 26, 2010

For: Kevin C. Ecker
Registration No.: 43,600
Phone: (914) 333-9618

Please direct all correspondence to:
Kevin C. Ecker, Esq.
Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001